Introduction To IT

Lecture 5

Fall Semester

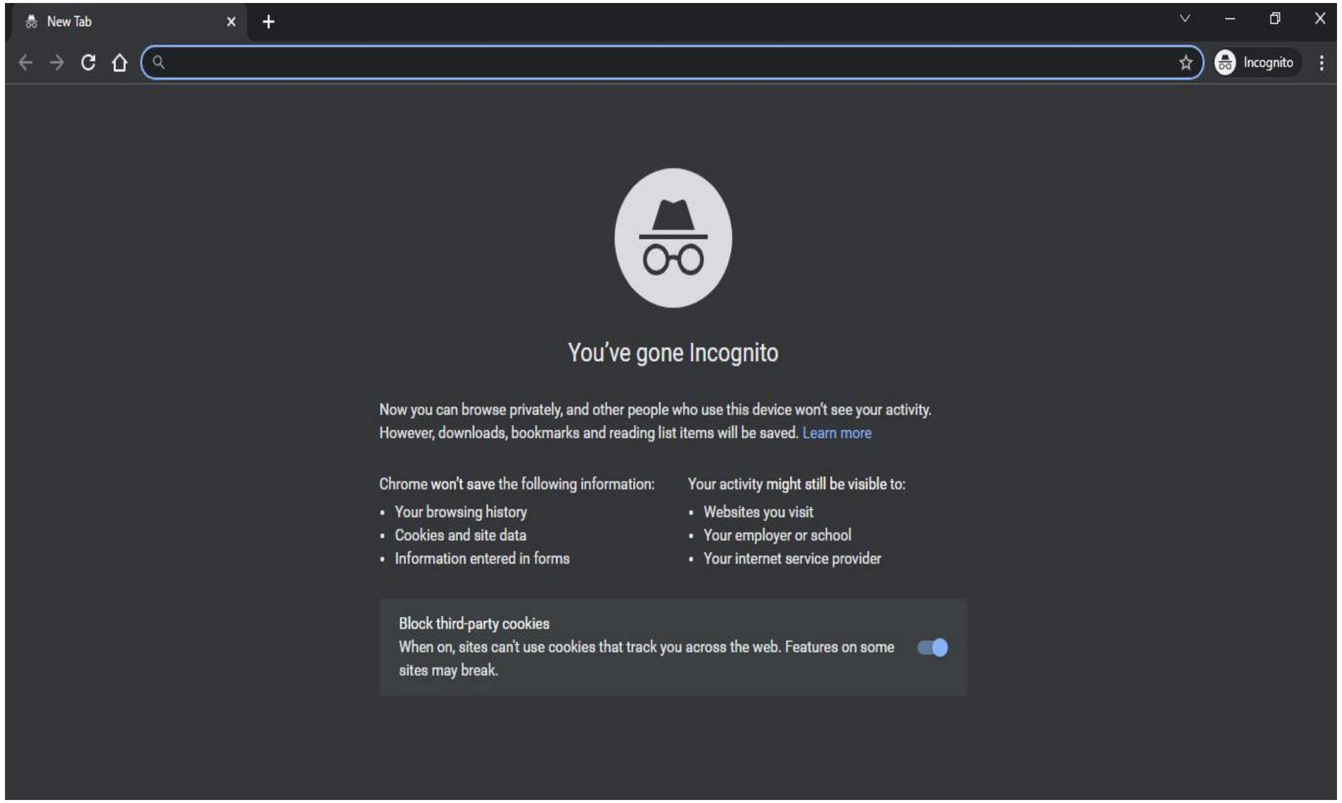
Lecturer: M.Sc. Goran N. Saleh

Privacy Modes

- Most browsers also offer a **privacy mode**, which ensures that your browsing activity is not recorded on your hard disk.

For example

- **Google Chrome** provides **Incognito Mode** accessible from the Chrome menu.
- **Safari** provides **Private Browsing** accessible from the Safari option on the main menu.



You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

Privacy Modes

Privacy mode: eliminates history files as well as blocks most cookies.

Incognito mode: privacy mode for Chrome

Private Browsing: privacy mode for Safari

Privacy Threats

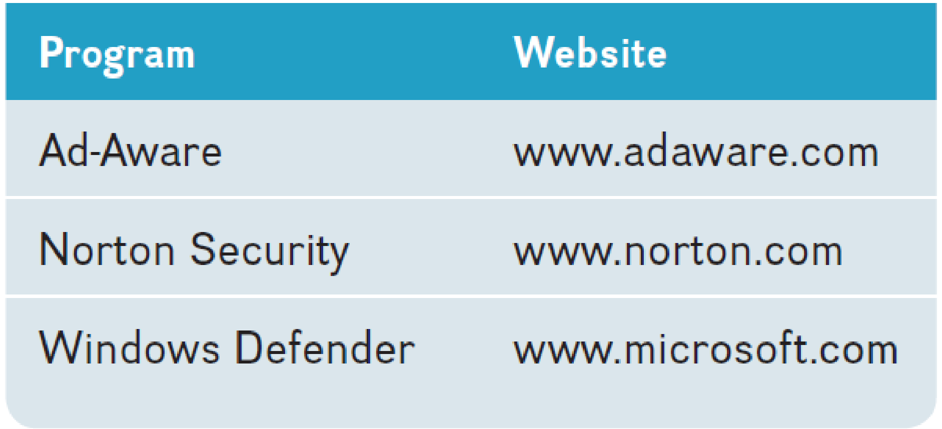
- **Web bugs**
  - Web bugs are invisible images or HTML code hidden within an e-mail message or web page
- **Spyware**
  - Spyware is the most dangerous type of privacy threat
  - Spyware is secretly record and report the internet activities of an individual’s.
  - Spyware can change browser to manipulate what you see online

Privacy Threats

- **Computer monitoring software**
    - Most dangerous type of spyware
    - Programs record every activity and keystroke made on a computer system including credit card numbers, bank account numbers, and e-mail messages
    - Keystroke Loggers - can be deposited on a hard drive without detection from the Web or by someone installing programs directly onto a computer
        - Record activities and keystrokes

Privacy Threats

- **Anti-Spyware programs / spy removal programs**
  - Detect and remove privacy threats
  - A category of programs known as spy removal programs designed to detect Web bugs and monitoring software



Program	Website
Ad-Aware	www.adaware.com
Norton Security	www.norton.com
Windows Defender	www.microsoft.com

Figure . **Antispyware programs**

Online Identity

Online identity: can be defined as the information that people voluntarily post about themselves online

- Archiving and search features of the Web make it available indefinitely

Online Identity

- **Major Laws on Privacy related to the online identity**
  1) **Gramm-Leach-Bliley Act** protects personal financial information
  2) **Health Insurance Portability and Accountability Act (HIPAA)**
     - protects medical records
  3) **Family Educational Rights and Privacy Act (FERPA)** resists disclosure of educational records

Concept check

1) Define history files
2) Define temporary Internet files/ Browser Cache
3) Define Privacy mode
4) What is a cookie? A first-party cookie? A third-party cookie?
5) What is a web bug? Spyware? Keystroke Loggers ? Antispyware programs? Online identity?
6) Describe three federal laws to protect privacy.

Concept check

8) List the two basic types of cookies

9) Define Incognito mode

10) Define Private Browsing

11) List the major laws on privacy related to the online identity and explain one of them in detail.

Security

Security: Involves protecting individuals or organizations from theft and danger.

- People who gain unauthorized access to computers are hackers
- Not all hackers are illegal

Cybercrime / Computer Crime: can be defined as the criminal offense that involves a computer and a network

- Effects over 400 million people annually
- Costs over $400 billion each year

Forms of Computer Crime

List some of the most common forms of Computer Crime

Computer Crime	Description
1) Identity theft	Illegal assumption of a person’s identity for economic gain
2) Internet scams	Scams over the Internet
3) Data manipulation	Unauthorized access of a computer network and copying files to or from the server
4) Ransomware	Malicious software that encrypts your computer’s data and ransoms the password to the user
5) DoS, Denial of service	Attempts to slow down or stop a computer system or network by flooding a computer or network with requests for information and data

Internet Scams

Internet scams are scams using the Internet.

- Internet scams have created financial and legal problems for many thousands of people
- Majority are initiated by a mass mailing to unsuspecting individuals

Common Internet Scams

Lists some of the most common Internet Scams:

1) Advance fee loans
2) Auction fraud
3) Fake antivirus software
4) Nigerian Scam

Common Internet Scams

Lists some of the most common Internet Scams

Type	Description
1) Advance fee loans	Guaranteed low-rate loans available to almost anyone. After applicant provides personal loan-related information, the loan is granted subject to payment of an “insurance fee.”
2) Auction fraud	Merchandise is selected and payment is sent. Merchandise is never delivered.
3) Fake antivirus software	A website or e-mail warns you that you are at risk of being infected by a computer virus and you need to download and install the security software they recommend. The security software is fake and will install malicious software on your computer.
4) Nigerian Scam	A classic e-mail scam. The recipient receives an e-mail from a wealthy foreigner in distress who needs your bank account information to safely store their wealth, and for your troubles you will receive a large amount of money. Of course, once the scammer has your bank account information, your accounts will be drained and they will disappear

Concept check

1) Define security, hackers.
2) What is cybercrime?
3) List some of the most common forms of computer crime and explain one of them in detail.
4) What are identity theft and Internet scams?
5) What are data manipulation, ransomware, and denial of service attacks?
6) Lists some of the most common Internet Scams and explain one of them in detail.

Social Engineering

Social engineering is the practice of manipulating people to divulge private data.

Played a key role in:

1) Identity theft
2) Internet scams
3) Data manipulation

Social Engineering

- The most common social engineering technique is Phishing
- Phishing can be defined as the attempts to trick Internet users into thinking a fake but official-looking website or e-mail is legal.

Malicious Programs - Malware

- **Malicious Programs or Malware**
  - Malicious Programs or Malware designed by crackers (computer criminals) to damage or disrupt a computer system
  - Computer Fraud and Abuse Act makes spreading a virus a federal offense
  - **The three most common Malicious Programs / Malware**
    1) Viruses – migrate through networks and attach to different programs; can alter and/or delete files; can damage system components.
    2) Worms – a special type of virus fills the computer with self-replicating information
    3) Trojan horse – programs disguised as something else; The most common type of Trojan horses appear as free computer games.

Malicious Hardware

Criminals use hardware for crimes.

Most common malicious hardware are:

1) **Zombies**
2) **Rogue Wi-Fi Hotspots**
3) **Infect USB Flash Drives**

Malicious Hardware

Cyber criminals can use computer hardware to steal information.

Three types of malicious hardware:

1) Zombies

- **Zombies** are computers infected by a virus, worm, or Trojan Horse that allows them to be remotely controlled for malicious purposes.
- Botnet or Robot Network is a collection of Zombies

Malicious Hardware

Cyber criminals can use computer hardware to steal information.

Three types of malicious hardware:

2) **Rogue Wi-Fi Hotspots**

Imitate a legitimate free Wi-Fi hotspot. When users connect to this rogue Wi-Fi, their data and private information is captured and used for illegal activities

Malicious Hardware

Cyber criminals can use computer hardware to steal information. Three types of malicious hardware:

3) **Infect USB Flash Drives**

- Crackers load malicious software on the USB drives and left on purpose in hopes for people to pick up and use.
- Infect USB flash drives have malicious software contained on them.

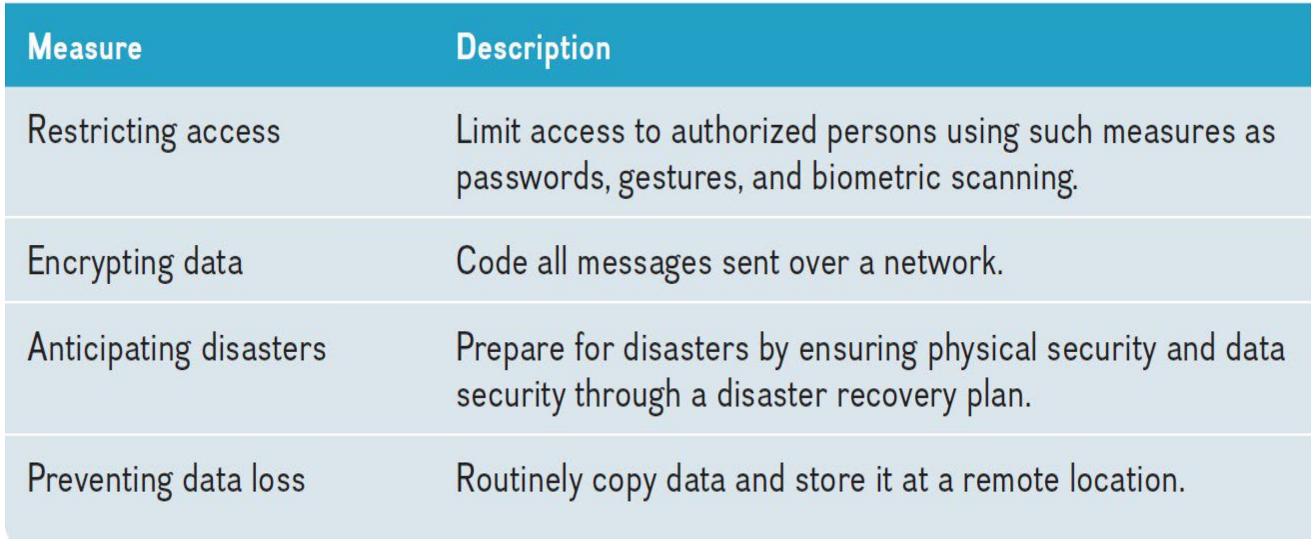
Concept check

1) What is social engineering? What is phishing?
2) What is malicious Programs / Malware
3) List the three most common Malicious Programs / Malware and explain one of them in detail.
4) Define Viruses, Worms, and Trojan horses.
5) What is malicious hardware? Zombies? Botnets? Rogue Wi-Fi hotspots? Infected USB flash drives?
6) List the three types of malicious hardware and explain one of them in detail.

Measures to Protect Computer Security

Principle measures to ensure computer security

- **Computer Fraud and Abuse Act**
  - Crime for unauthorized person to view, copy or damage data using computers across state lines
  - Prevents use of any government or federally insured financial institution computers



Measure	Description
Restricting access	Limit access to authorized persons using such measures as passwords, gestures, and biometric scanning.
Encrypting data	Code all messages sent over a network.
Anticipating disasters	Prepare for disasters by ensuring physical security and data security through a disaster recovery plan.
Preventing data loss	Routinely copy data and store it at a remote location.

Restricting Access

- Computers should be protected from unauthorized access by using **Passwords** or **Biometric scanning devices**

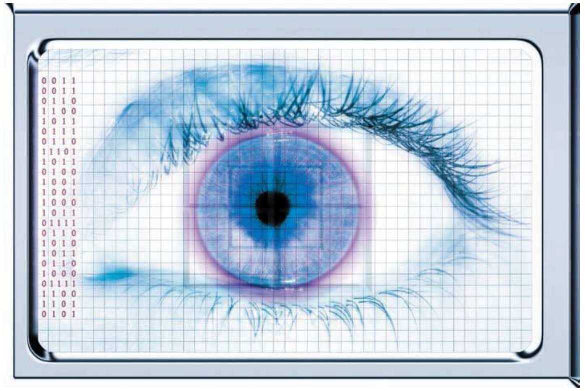
Passwords: is the most common way to restrict access

- **Dictionary attack**

  Uses software to try thousands of common words sequentially in an attempt to gain unauthorized access to a user's account

Restricting Access

- Computers should be protected from unauthorized access
- Biometric scanning devices such as Fingerprint scanners and Iris (eye) scanners
- Facial recognition (technology that recognizes your face and logs you into your computer)



Thank You